

19. Функция Эйлера: значение на степени простого числа, явный вид

Функция Эйлера

Лемма 4

Функция Эйлера **мультипликативна**, то есть, если $a, b \in \mathbb{N}$ взаимно просты, то $\varphi(ab) = \varphi(a)\varphi(b)$.

Доказательство. • Запишем числа от 1 до ab в таблицу $a \times b$ так, что в первой строке — числа от 1 до a , во второй — от $a+1$ до $2a$, итд, в b строке — числа от $(b-1)a+1$ до ba .

1	2	3	...	a-3	a-2	a-1	a
a+1	a+2	a+3	...	2a-3	2a-2	2a-1	2a
...							
(b-1)a+1	(b-1)a+2	(b-1)a+3	...	ba-3	ba-2	ba-1	ba



b строк

- Все числа в i столбце принадлежат одному вычету $\bar{i} = i + a\mathbb{Z}$ по модулю a . Эти числа взаимно просты с a , если и только если $(i, a) = 1$.
- Вычеркнем все столбцы с номерами i , не взаимно простыми с a . Останутся ровно $\varphi(a)$ столбцов.

Пусть $a = 8$; $b = 3$.

PS функция Эйлера от 8 это 4 (нам подходят 1, 3, 5, 7)

функция Эйлера от 3 это 2 (нам подходят 1, 2)

функция Эйлера от 24 это 8 (нам подходят 1, 5, 7, 11, 13, 15, 17, 19)

1	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24
ПСВ 3		ПСВ 3		ПСВ 3		ПСВ 3	

То есть в этой табличке мы получили все варианты остатков по модулю ab .

- Все числа, взаимно простые с ab , должны быть взаимно простыми и с a , они лежат в оставшихся $\varphi(a)$ столбцах.
- Рассмотрим оставшийся столбец, пусть числа в нем имеют вид $j, a+j, \dots, (b-1)a+j$. Эти числа образуют ПСВ $(\text{mod } b)$ в силу теоремы 13 (так как получены из ПСВ $0, 1, \dots, b-1$ умножением на a , взаимно простое с b и прибавлением j : $0 \rightarrow j, 1 \rightarrow a+j, \dots, b-1 \rightarrow (b-1)a+j$).

- Значит, среди чисел $j, a+j, \dots, (b-1)a+j$ ровно $\varphi(b)$ взаимно простых с b . Остальные числа точно не взаимно просты с ab , вычеркнем их.
- Оставшиеся $\varphi(a)\varphi(b)$ чисел взаимно просты и с a , и с b , а значит, взаимно просты с ab . Значит, осталось ровно $\varphi(ab)$ чисел (все числа от 1 до ab , взаимно простые с ab). \square

1	2	3	4	5	6	7	8
9	10	11	12	13	14	15	16
17	18	19	20	21	22	23	24
ПСВ 3		ПСВ 3		ПСВ 3		ПСВ 3	

Лемма 5

Если $p \in \mathbb{P}$, $n \in \mathbb{N}$, то $\varphi(p^n) = p^n - p^{n-1}$.

Доказательство. • Посчитаем количество чисел от 1 до p^n , не взаимно простых с p^n .

- Пусть $(a, p^n) = d > 1$. Так как $p^n \vdots d$, должно быть $d \vdots p$.
- Следовательно, числа от 1 до p^n , не взаимно простые с p^n — это в точности числа от 1 до p^n , кратные p . Их количество равно $\frac{p^n}{p} = p^{n-1}$. \square

Комментарии: действительно, что у нас может быть не взаимно простого с простым числом в какой-то степени? Собственно, все числа, кратные p (то есть каждое p -тое). Их как раз p^{n-1} .

Теорема 16

Если $n \in \mathbb{N}$ имеет каноническое разложение $n = p_1^{k_1} \dots p_m^{k_m}$, то

$$\varphi(n) = n \left(1 - \frac{1}{p_1}\right) \dots \left(1 - \frac{1}{p_m}\right).$$

Доказательство. • Докажем индукцией по количеству простых делителей s , что $\varphi(p_1^{k_1} \dots p_s^{k_s}) = \prod_{i=1}^s \varphi(p_i^{k_i})$.

- База для $s = 1$ очевидна.
- **Переход $s \rightarrow s+1$.** Так как $(p_1^{k_1} \dots p_s^{k_s}, p_{s+1}^{k_{s+1}}) = 1$, по Лемме 4 и индукционному предположению имеем

$$\begin{aligned} \varphi(p_1^{k_1} \dots p_s^{k_s} \cdot p_{s+1}^{k_{s+1}}) &= \varphi(p_1^{k_1} \dots p_s^{k_s}) \cdot \varphi(p_{s+1}^{k_{s+1}}) = \\ &= \left(\prod_{i=1}^s \varphi(p_i^{k_i}) \right) \cdot \varphi(p_{s+1}^{k_{s+1}}) = \prod_{i=1}^{s+1} \varphi(p_i^{k_i}). \end{aligned}$$

- Следовательно,

$$\varphi(n) = \prod_{i=1}^m \varphi(p_i^{k_i}) = \prod_{i=1}^m (p_i^{k_i} - p_i^{k_i-1}) = \prod_{i=1}^m p_i^{k_i} \left(1 - \frac{1}{p_i}\right) = n \cdot \prod_{i=1}^m \left(1 - \frac{1}{p_i}\right).$$

Сумма функции Эйлера по делителям числа

Теорема 17

Для любого $n \in \mathbb{N}$
$$\sum_{d \in \mathbb{N}, d \mid n} \varphi(d) = n.$$

Давайте немного посмотрим на примерах: пусть $n = 12$. Тогда сумма будет равна $\varphi(1) + \varphi(2) + \varphi(3) + \varphi(4) + \varphi(6) + \varphi(12) = 1+1+2+2+2+4 = 12$

$n = 14$. Тогда сумма будет равна $\varphi(1) + \varphi(2) + \varphi(7) + \varphi(14) = 1+1+6+6 = 14$

Пусть $n = 13$. Тогда $\varphi(1) + \varphi(13) = 13$

Доказательство. • Рассмотрим все \mathbb{N} числа от 1 до n — их как раз n штук. Каждое из них имеет НОД с n — и этот НОД — делитель n .

• Для любого $d \mid n$ подсчитаем количество всех чисел из $\{1, \dots, n\}$, чей НОД с n равен d .

Число 14. Хотим для каждого делителя d посмотреть, сколько $(\{1, \dots, n\}, n)=d$. То есть для 14:

$14 = 1 \cdot 2 \cdot 7$, делители 14 — это 1, 2, 7, 14.

$(\{1, \dots, 14\}, 14) = 1$, это выполняется для 1, 3, 5, 9, 11, 13, то есть таких 6 штук.

$(\{1, \dots, 14\}, 14) = 2$, это выполняется для 2, 4, 6, 8, 10, 12, то есть таких 6 штук.

$(\{1, \dots, 14\}, 14) = 7$, это выполняется для 7, то есть таких 1 штука.

$(\{1, \dots, 14\}, 14) = 14$, это выполняется для 14, то есть таких 1 штука.

• Такие числа делятся на d , значит, их нужно искать среди $d, 2d, \dots, n = \frac{n}{d}d$. Так как

$$d = (kd, n) = (kd, \frac{n}{d}d) = d \cdot (k, \frac{n}{d}) \iff (k, \frac{n}{d}) = 1,$$

количество чисел из $\{1, \dots, n\}$, чей НОД с n равен d — это в точности количество таких $k \in \{1, \dots, \frac{n}{d}\}$, что $(k, \frac{n}{d}) = 1$, а это количество равно $\varphi(\frac{n}{d})$.

$k \in \{1, 2, 7, 14\}$

$$\varphi(1) + \varphi(2) + \varphi(7) + \varphi(14) = 14$$

• Если d пробегает все натуральные делители n , то $d' = \frac{n}{d}$ также пробегает все натуральные делители n . Поэтому,

$$n = \sum_{d \in \mathbb{N}, d \mid n} \varphi(\frac{n}{d}) = \sum_{d' \in \mathbb{N}, d' \mid n} \varphi(d').$$



Другой вариант доказательства:

1 Случай: если n – простое число, то делители n – это 1 и, собственно, n . Тогда $\varphi(1) + \varphi(n) = n$.

2 Случай: если n – составное число, $n = p_1^{\alpha_1} * p_2^{\alpha_2} * p_3^{\alpha_3} * p_4^{\alpha_4} * \dots * p_s^{\alpha_s}$ (каноническое разложение)

Заметим одну интересную вещь:

$$\varphi(1) + \varphi(p) + \varphi(p^2) + \varphi(p^3) + \dots + \varphi(p^l) = 1 + (p - p^0) + (p^2 - p) + (p^3 - p^2) + \dots + (p^l - p^{l-1})$$

Телескоп ☺, останется только p^l .

$$n = (\varphi(1) + \varphi(p_1) + \varphi(p_1^2) + \dots + \varphi(p_1^{\alpha_1})) * (\varphi(1) + \varphi(p_2) + \varphi(p_2^2) + \dots + \varphi(p_2^{\alpha_2})) * \dots * (\varphi(1) + \varphi(p_s) + \varphi(p_s^2) + \dots + \varphi(p_s^{\alpha_s}))$$

Если раскрыть скобки, будут получаться слагаемые вида $\varphi(p_i) * \varphi(p_j) * \dots * \varphi(p_q)$, но вследствие мультипликативности функции Эйлера получим $\varphi(p_i * p_j * p_q)$, где произведение p -шек это делитель n .

21. Кольцо вычетов и его обратимые элементы. Поле вычетов по простому модулю.

Кольцо вычетов

- Вычеты по модулю $m \in \mathbb{Z}$ — они же вычеты по модулю идеала $m\mathbb{Z}$ — образуют **кольцо вычетов** $\mathbb{Z}_m := \mathbb{Z}/m\mathbb{Z}$.

Лемма 6

Обратимые элементы \mathbb{Z}_m — это в точности вычеты из ПрСВ $(\text{mod } m)$.

ПрСВ – приведённая система вычетов, например: $m = 42$. Тогда приведенная система вычетов: 1, 5, 11, 13, 17, 19, 23, 25, 29, 31, 37, 41. (то есть числа из полной системы вычетов, но взаимно простые с m)

Доказательство. • Если $\bar{a} \in \mathbb{Z}_m$ обратим, то существует такой $\bar{b} \in \mathbb{Z}_m$, что $\bar{a}\bar{b} = \bar{1} \iff ab \equiv_m 1$. Тогда $(ab, m) = 1$, а значит и $(a, m) = 1$.

- Наоборот, пусть $(a, m) = 1$. По Теореме 13 тогда $0, a, 2a, \dots, (m-1)a$ — ПСВ $(\text{mod } m)$. Значит, $\exists b : ab \equiv_m 1 \Rightarrow \bar{a}\bar{b} = \bar{1}$. □

Комментарии: как мы знаем, (наверное, привет сравнению по модулю идеала). Если ab и m отличаются на 1, то, конечно, они взаимно простые. Если выкинем b , никаких новых делителей точно не появится, поэтому НОД останется 1. Вот мы и получили, что \bar{a} это вычет из ПрСВ $(\text{mod } m)$


(обратим, если имеет обратный)

- Если вычет \bar{a} обратим, то обратный вычет $(\bar{a})^{-1}$ единственен (это доказано в общем случае для кольца ранее, а в данном случае следует из доказательства Леммы 6).

Теорема 18

Если $p \in \mathbb{P}$, то \mathbb{Z}_p — поле.

Доказательство. Так как все некрратные p числа взаимно просты с p , ПрСВ $(\text{mod } p)$ — это все ненулевые вычеты.

Тогда по Лемме 6, все ненулевые элементы \mathbb{Z}_p обратимы. 

Про кольцо нам уже сказали выше. Что нам не хватает для поля? Обратного элемента по умножению. А мы знаем, что ненулевые элементы обратимы.

Алгоритм поиска обратного вычета

- Пусть $a \in \mathbb{Z}$, $m \in \mathbb{N}$, причем $(a, m) = 1$. Как найти обратный вычет a^{-1} ?
- Пусть r — остаток от деления a на m . Тогда $0 \leq r < m$.

$$a = km + r$$

Пусть у нас есть кольцо по модулю 26. Тогда ПрСВ: 1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25.

Обратный вычет к 1 — это 1, 3 — это 9, 5 — это 21 и тд

$$m = 26$$

- Если $r = 0$, то $(a, m) > 1$ и обратного вычета не существует.
- Если $r > 0$, то с помощью алгоритма Евклида ищем $d = (r, m) = (a, m)$.

$$55 = 2 \cdot 26 + 3, d = (3, 26) = 1$$

$$54 = 2 \cdot 26 + 2, d = (54, 26) = 2, \text{ то есть к } 54 \text{ нет обр вычета}$$

$$1 = 55 \cdot x + 26y, x=9, y=-19 \text{ (как частный случай решения)}$$

$$55 \cdot 9 \equiv 1 \pmod{26} \text{ (х это и есть вычет)}$$

- Если $d > 1$, то обратного вычета не существует.
- Если $d = 1$, то при помощи (выполненного ранее) алгоритма Евклида ищем линейное представление НОД: $1 = ax + my$.
- Тогда $ax \equiv 1 \pmod{m}$, а значит, $(\bar{a})^{-1} = \bar{x}$ в \mathbb{Z}_m .

Линейное сравнение с одним неизвестным

Алгебра. Глава
2. Целые числа

Д. В. Карпов

- Пусть $a, b \in \mathbb{Z}$, $m \in \mathbb{N}$. Нужно решить (относительно x) сравнение

$$ax \equiv b \pmod{m}. \quad (*)$$

- Пусть $d = (a, m)$. Если $b \not\vdots d$, то очевидно, $(*)$ решений не имеет.

- Если $b \vdots d$, то пусть $a = a'd$, $b = b'd$, $m = m'd$. Тогда

$$(*) \iff ax - b \vdots m \iff a'x - b' \vdots m' \iff a'x \equiv b' \pmod{m'}. \quad (**)$$

- Так как $(a', m') = 1$, существует обратный вычет $(\overline{a'})^{-1}$ в $\mathbb{Z}_{m'}$.

- Пусть $s \in (\overline{a'})^{-1}$. Тогда $x \equiv b's \pmod{m'}$ — решение сравнения $(**)$, а значит, и исходного сравнения $(*)$.

$$5x \equiv 15 \pmod{10}$$

$$6x \equiv 7 \pmod{2}$$

$$d = (5, 10) = 5$$

$$d = (6, 2) = 2, 7 \text{ на } 2 \text{ не делится, ежу понятно, что решений нет}$$

Дальше сокращаем на d :

$$x \equiv 3 \pmod{2}$$

$(1, 2) = 1$, существует обратный вычет для 1 в \mathbb{Z} по m' , то есть по 2. Это 1 в нашем случае. Тогда $x \equiv 3 * 1 \pmod{2}$ — наше решение.

Алгоритмы поиска решения для КТО

- Пусть m_1, \dots, m_k — попарно взаимно простые натуральные числа, $m = m_1 \dots m_k$, $a_1, \dots, a_k \in \mathbb{Z}$.
- Мы ищем такое a , что $a \equiv_{m_1} a_1, \dots, a \equiv_{m_k} a_k$ (*).
- Будет использоваться алгоритм поиска обратного вычета, описанный выше.

Алгоритм 1.

- Пусть $m'_i = \frac{m_1 \dots m_k}{m_i}$. Тогда $(m'_i, m_i) = 1$.
 $b_i \in \{0, 1, \dots, m_i - 1\}$ — такое число, что $b_i \cdot m'_i \equiv 1 \pmod{m_i}$ (мы найдем b_i с помощью алгоритма поиска обратного вычета).

Утверждение

$a = a_1 b_1 m'_1 + a_2 b_2 m'_2 + \dots + a_k b_k m'_k$ — решение (*).

$$m_1 = 8; m_2 = 11; m_3 = 15$$

$$m = 8 * 11 * 15 = 1320$$

$$a \equiv a_1 \pmod{8}; a \equiv a_2 \pmod{11}; a \equiv a_3 \pmod{15}$$

$$a_1 = 7; a_2 = -1; a_3 = 3$$

$$a \equiv 7 \pmod{8}; a \equiv -1 \pmod{11}; a \equiv 3 \pmod{15}$$

b_i — это фактически обратный вычет к m'_i по модулю m_i

$$m'_1 = \frac{8 * 11 * 15}{8} = 165; m'_2 = \frac{8 * 11 * 15}{11} = 120; m'_3 = \frac{8 * 11 * 15}{15} = 88$$

$$b_1 = 5; b_2 = 10; b_3 = 7$$

$$a = 7 * 5 * 165 - 10 * 120 + 3 * 7 * 88 = 6423$$

И вы не поверите! Это действительно работает!!

Тогда ответ имеет вид: $x \equiv 6423 \pmod{1320} = 1143 \pmod{1320}$

Ответ: $x \equiv 1143 \pmod{1320}$

Доказательство. Так как $m'_j \vdots m_i$ при всех $j \neq i$, для любого $i \in \{1, \dots, k\}$

$$a \equiv a_i; b_i m'_i \equiv a_i \pmod{m_i}.$$



- Как сказано выше, все решения системы (*) — это в точности числа, сравнимые с a по модулю m .

- Поделив a на m с остатком, мы найдем решение системы среди чисел $0, 1, \dots, m - 1$.

Алгоритм 2

- Индукцией по s найдем x_s , удовлетворяющее первым s сравнениям:

$$x_s \equiv_{m_1} a_1, \dots, x_s \equiv_{m_s} a_s.$$

- База $s = 1$ очевидна: подойдет $x_1 = a_1$.

Переход $s \rightarrow s + 1$. • Пусть $n_s = m_1 \dots m_s$.

Будем искать решение в виде $x_{s+1} = x_s + c_s n_s$.

- Тогда $x_{s+1} - x_s \equiv m_j$ для всех $j \in \{1, \dots, s\}$, поэтому, x_{s+1} удовлетворяет первым s сравнениям.

- Подберем c_s так, чтобы $x_{s+1} \equiv a_{s+1} \pmod{m_{s+1}}$:

$$\begin{aligned} x_s + c_s n_s &\equiv a_{s+1} \pmod{m_{s+1}} \iff c_s n_s \equiv a_{s+1} - x_s \pmod{m_{s+1}} \\ &\iff c_s \equiv (a_{s+1} - x_s) \cdot (n_s)^{-1} \pmod{m_{s+1}}. \end{aligned}$$

- Так как $(n_s, m_{s+1}) = 1$, обратный вычет $(n_s)^{-1}$ существует и может быть найден с помощью описанного выше алгоритма.

- Второй алгоритм решения КТО на первый взгляд сложнее, чем первый, но требует применения $k - 1$ алгоритмов поиска обратного вычета (а не k): мы не ищем обратный вычет по модулю m_1 .

- Поэтому, целесообразно нумеровать модули так, чтобы m_1 оказался самым большим.



Комментарии:

тут фишка в чём: решения мы подбираем последовательно. То есть методом пристального взгляда нашли какой-то x_s , который удовлетворяет первым s сравнениям. А потом пошли дальше подбирать, чтобы при этом ничего предыдущего не испортить.

a) $x \equiv 3 \pmod{8}, x \equiv 1 \pmod{11}, x \equiv 12 \pmod{15};$

Во-первых, перенумеруем m -ки:

$$m_1 = 15; m_2 = 11; m_3 = 8$$

$a_1 = 12; a_2 = 1; a_3 = 3$, то есть система имеет вид

$$\begin{cases} x \equiv 12 \pmod{15} \\ x \equiv 1 \pmod{11} \\ x \equiv 3 \pmod{8} \end{cases}$$

$$x_1 = 12; n_1 = 15$$

$$x_2 = x_1 + c_1 * n_1 = 12 + c_1 * 15$$

Подберём c_1 : $x_2 \equiv a_2 \pmod{m_2}$; то есть $x_2 \equiv 1 \pmod{11}$:

$$12 + 15c_1 \equiv 1 \pmod{11}; \quad 15c_1 \equiv -11 \pmod{11}; \quad c_1 \equiv -11 * 15^{-1} \pmod{11}$$

Вычет 15 по модулю 11: 3, то есть имеем

$$c_1 \equiv -33 \pmod{11}, \text{ откуда } c_1 = 0.$$

$x_2 = 12$. Повторим алгоритм:

$$x_3 = x_2 + c_2 * n_2, \text{ где } n_2 = m_1 * m_2, \text{ в нашем случае } n_2 = 165; \quad x_3 = 12 + 165c_2.$$

$$\text{Подберём } c_2: \quad x_3 \equiv a_3 \pmod{m_3}, \text{ то есть } x_3 \equiv 3 \pmod{8}; \quad 12 + 165c_2 \equiv 3 \pmod{8};$$

$$165c_2 \equiv -9 \pmod{8}; \quad c_2 \equiv 165^{-1} * (-9) \pmod{8}; \quad c_2 \equiv -45 \pmod{8}; \quad c_2 \equiv 3 \pmod{8}$$

$$x_3 = 12 + 3 * 165 = 507, \text{ подходит}$$

$$\text{Ответ: } \quad x \equiv 507 \pmod{1320}$$

Функция Мёбиуса

Определение

Функция Мёбиуса

$$\mu(n) := \begin{cases} 1, & \text{если } n = 1, \\ (-1)^k, & \text{если } n = p_1 \dots p_k \text{ — произведение различных простых чисел,} \\ 0, & \text{если } n \text{ делится на квадрат простого числа.} \end{cases}$$

Лемма 8

Пусть $m, d \in \mathbb{N}$, $m \vdots d$. Тогда $\sum_{d|n|m} \mu\left(\frac{m}{n}\right) = \begin{cases} 1, & m = d, \\ 0, & m > d. \end{cases}$

(суммирование ведется по всем n , кратным d и делящим m).

То есть если по-русски: $\left\{ \begin{matrix} m \vdots n \\ n \vdots d \end{matrix} \right\}$ $m=kd$ (из условия m делится на d)

Доказательство. • Пусть $k := \frac{m}{d} = p_1^{t_1} \dots p_r^{t_r}$ — каноническое разложение. Тогда

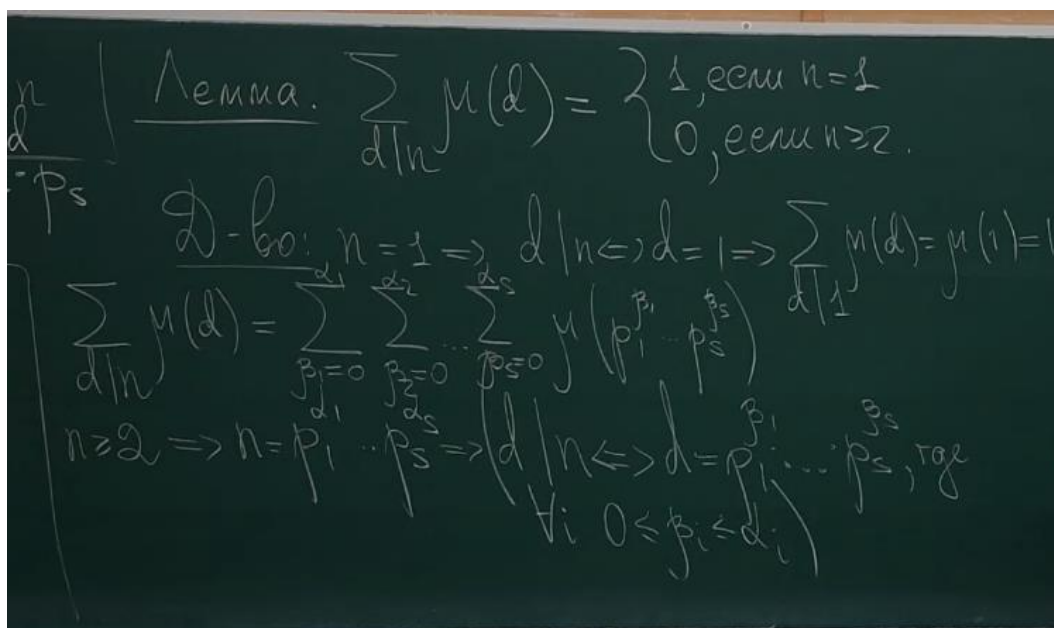
$$\sum_{d|n|m} \mu\left(\frac{m}{n}\right) = \sum_{s|p_1 \dots p_r} \mu(s) = \sum_{\ell=0}^r C_r^\ell (-1)^\ell = (1-1)^r$$

(так как ненулевое значение μ достигается только на произведениях различных простых).

• Наша сумма равна 0 во всех случаях, кроме $r = 0$ (а это в точности $k = 1 \iff m = d$). В последнем случае сумма равна 1.



Вы что-нибудь поняли? Я – нет. Поэтому вот альтернативное доказательство:



$$\sum_{\beta_1=0}^1 \dots \sum_{\beta_s=0}^1 \mu(p_1^{\beta_1} \dots p_s^{\beta_s}) = C_s^0 - C_s^1 + C_s^2 - \dots + (-1)^s C_s^s = 0$$

Эта страшная сумма – для каждого фиксированного набора вычисляем значение μ , потом переходим к варианту, где β только 0 или 1 (остальное рассматривать бессмысленно – оно обращается в 0). А потом рассматриваем варианты сумм: сначала набор, где все β равны 0. Такой набор единственный, представляется в виде C_s^0 . Потом рассматриваем вариант, где только одна β единичка. Таких вариантов C_s^1 . При этом функция Мёбиуса будет -1. И ему понятно, что эта сумма зануляется ☺

27. Формула обращения Мёбиуса, аддитивный вариант.

Формула обращения Мёбиуса. Аддитивный вариант

Теорема 20

Пусть $f, g : \mathbb{N} \rightarrow \dots$, причем $f(m) = \sum_{d|m} g(d)$. Тогда

$$g(m) = \sum_{n|m} \mu\left(\frac{m}{n}\right) f(n).$$

Доказательство.

$$\begin{aligned} \sum_{n|m} \mu\left(\frac{m}{n}\right) f(n) &= \sum_{n|m} \mu\left(\frac{m}{n}\right) \cdot \sum_{d|n} g(d) = \\ &= \sum_{d|m} \left(g(d) \cdot \sum_{d|n|m} \mu\left(\frac{m}{n}\right) \right) = g(m) \end{aligned}$$

по Лемме 8. □

Т. (Ф-на обращения Миссуры). Пусть $f(n)$ - Ф-ция от $n \in \mathbb{N}$. Пусть $g(n) = \sum_{d|n} f(d)$. Тогда $f(n) = \sum_{d|n} \mu(d) \cdot g\left(\frac{n}{d}\right) = \sum_{d|n} \mu\left(\frac{n}{d}\right) \cdot g(d)$

(нет разницы, в каком порядке брать делители n)

$$\sum_{d|n} \mu(d) \cdot g\left(\frac{n}{d}\right) = \sum_{d|n} \mu(d) \cdot \left(\sum_{d'|\frac{n}{d}} f(d') \right)$$

Лемма. $\sum_{d|n} \mu(d) = \begin{cases} 1, & \text{если } n=1 \\ 0, & \text{если } n \geq 2 \end{cases}$

$$\begin{aligned} \sum_{(d,d'): dd'|n} \mu(d) \cdot f(d') &= \sum_{d|n} f(d) \cdot \left(\sum_{d'|\frac{n}{d}} \mu(d') \right) = \\ &= f(n) \cdot 1 + \sum_{\substack{d|n \\ d < n}} f(d) \cdot \underbrace{\left(\sum_{d'|\frac{n}{d}} \mu(d') \right)}_0 = f(n). \end{aligned}$$